

UNITED STATES DISTRICT COURT

JUN 16 2017

for the
Southern District of Texas

David J. Bradley, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)One (1) Apple iPhone Model A1687, IMEI#
355729075698832 and Serial Number:
F2LT5ATSHFM5, rose gold in color

Case No.

B-17-554-MJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
One (1) Apple iPhone Model A1687, IMEI# 355729075698832 and Serial Number: F2LT5ATSHFM5, rose gold in color currently detained at the Homeland Security office located at 1717 Zoy Street in Harlingen, Texas.

located in the Southern District of Texas, there is now concealed (identify the person or describe the property to be seized):

(See Attachment A); Incoming Calls, Outgoing Calls, Missed Calls, Contact Directory, Voicemail and Text Messages, Photographs and/or Video, and any and all other electronic information stored on the phone or the SIM card inside the phone if the phone uses a SIM Card

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 922	Possession of a firearm by a prohibited person
22 U.S.C. 2778	Unlawful export of controlled defense articles

The application is based on these facts:
See Attached Sworn Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jesse Axley, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

June 16, 2017

City and state: Brownsville, Texas

Judge's signature

Ignacio Torteja, III, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

United States District Court
Southern District of Texas
FILED

JUN 16 2017

David J. Bradley, Clerk of Court

IN THE MATTER OF THE SEARCH OF

Apple iPhone
Model A1687
IMEI: 355729075698832
S/N: F2LT5ATSHFM5

Case No. B-17-554-mJ

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jesse Axley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search One (1) Apple iPhone Model A1687, IMEI# 355729075698832 and Serial Number: F2LT5ATSHFM5, rose gold in color, which was located and seized from Virginia Kimberly Aramburu on May 17, 2017. This cell phone is currently in the possession of Homeland Security Investigations Special Agent Jesse Axley assigned to the Homeland Security Investigations, Harlingen, TX (HSI/HG), Border Enforcement Security Task Force (BEST).

2. I am a Special Agent with the United States Department of Homeland Security, currently assigned to the Homeland Security Investigations in Harlingen, Texas. I have been so employed since 2015. My present responsibilities include the investigation of violations of Title 8, 18, 19, 21, and 31 of the United States Code and related offenses. I am authorized to conduct a wide range of law enforcement functions that deal with the violations of federal law, to include

export violations, in performance of my duties. As a Special Agent, I have received training in the investigation of Munitions trafficking and smuggling and violations of the ITAR, controlled substance smuggling and violations of the Controlled Substances Act, the Controlled Substances Import/Export Control Act, the Money Laundering Control Act, the Bank Secrecy Act and the Immigration and Naturalization Act.

3. Based upon my training, experience, and participation in arms and munitions trafficking investigations and investigations into the financial implications which result from violations of the ITAR, I know:

- a. That arms and munitions traffickers very often use wireless telephones to communicate, negotiate and coordinate illicit transactions with associates in relation to arms and munitions trafficking activities;
- b. That arms and munitions traffickers very often use wireless telephone capabilities to photograph arms and munitions and/or currency with the intention of sending photographs as attachments in text messaging or via electronic mail from their wireless telephones in an effort to prove possession of arms and munitions and or currency to associates;
- c. That arms and munitions traffickers commonly store phone numbers, direct connect numbers, electronic mail addresses, names and identities of associates in their wireless telephones;

- d. That arms and munitions traffickers commonly store photographs, text messages, electronic mail messages and other documents or information in their wireless telephone's memory in relation to violations of the ITAR;
- 4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

- 5. The following paragraphs are furnished to established probable cause in support of this warrant:
 - a. Affiant, in connection with an ongoing exportation of ITAR controlled items investigation, states that on May 17, 2017, Homeland Security Investigations, Harlingen, TX (HSI/HG), Border Enforcement Security Task Force (BEST) received information of a suspicious purchase at a local Federal Firearms Licensee (FFL) by a male subject, later identified as Emmanuel RAVELL, indicating RAVELL had purchased a large amount of AR-type rifle magazines which are restricted for export. RAVELL subsequently attempted to exit the United States via the Brownsville & Matamoros Port of Entry in Brownsville, TX in a Chevrolet Malibu occupied by four individuals. RAVELL was driving the vehicle, his girlfriend Virginia Kimberly Aramburu was in the front passenger seat, his cousin Tiffany (a minor) and Lizzette Alexis Capistran (a friend of his girlfriend) were in the back seat.

- b. Customs and Border Protection Officers (CBPOs) conducted an outbound inspection, and RAVELL gave a negative oral declaration for firearms, ammunition and monetary instruments in excess of \$10,000.00. CBPOs discovered a total of thirty (30) 5.56 x 45mm high capacity rifle magazines in a large Victoria Secret bag located in the vehicle in the floorboard of the front passenger seat occupied by Virginia Kimberly Aramburu. RAVELL admitted to purchasing the thirty (30) high capacity rifle magazines in order to export the aforementioned items into Mexico.
- c. The magazines purchased by RAVELL are controlled for export to Mexico under the provisions of the ITAR.
- d. Photographs from the security system were obtained from Academy Sporting Goods in Brownsville, TX showing RAVELL and Tiffany (a minor) at checkout, with RAVELL paying for the magazines.
- e. At the time of the encounter the iPhone for which this application for a search warrant has been submitted, hereto referred to as the Device, was in the possession of Virginia Kimberly Aramburu, and in a subsequent interview Virginia Kimberly Aramburu confirmed she was the owner of the cellular phone.
- f. During a routine search for merchandise of the Device conducted by HSI Special Agents pursuant to Border Search Authority as customs officers, photographs and videos depicting RAVELL firing and carrying firearms were discovered. Some of the photographs were geotagged showing they were taken at a firing range in

Brownsville, Texas. RAVELL is a convicted felon and as such is prohibited from possessing firearms.

- g. At the time of the encounter a ZTE cellular phone and a Samsung phone owned by RAVELL were discovered in the vehicle driven by RAVELL. An additional ZTE phone owned by Tiffany was in RAVELL's possession. Tiffany confirmed her ownership of the additional ZTE; however Tiffany stated RAVELL was the primary user of the ZTE. During a routine search for merchandise of the ZTE cellular phone conducted by HSI Special Agents pursuant to Border Search Authority as customs officers, conversations were observed that exhibited red flags for illicit purchase of firearms, straw purchases, and exportation of firearms.

6. The Device owned by Virginia Kimberly Aramburu is currently in the possession of Homeland Security Investigations Special Agents assigned to the HSI/HG, BEST.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls

made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store any digital data, such as word processing documents, even if the device is not designed to access such files. Some portable media players can use removable storage media.

Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs

usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on a device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

ELECTRONIC DEVICES AND STORAGE

9. As described above and in Attachment A, this application seeks permission to search and seize things that the Device might contain, in whatever form they are stored. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Device. This information can sometimes be recovered with forensics tools.

10. Searching for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas

unrelated to things described in Attachment A, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, Homeland Security Investigations intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

METHODOLOGY

11. Following the issuance of this warrant, I will collect and deliver the ~~subject cell~~ ^{Device} *JA* ~~phone~~ to wireless telephone forensic examiners. These examiners will attempt to power the Device, identify whether it is protected by a personal identification number (PIN), determine or circumvent the PIN and retrieve data from the Device. Unlike typical computers, many wireless telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the Device or in memory cards inserted into the Device. Current technology provides some solutions for acquiring some of the data stored in some wireless telephone models using forensic hardware and software. The forensic examiner will determine whether any data associated with this device may be so acquired and, if so, such data will be acquired forensically and the follow-on examination will be conducted using the forensic copy. Even if some of the stored information on the Device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must examine the Device manually and record the process and the results using digital photography. This process is time and labor intensive and, depending upon the workload of the few wireless telephone forensic examiners available, may take weeks or longer.

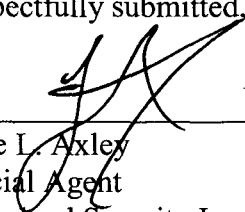
MANNER OF EXECUTION

12. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

13. I submit that this affidavit supports probable cause that evidence of violations of Title 18, United States Code, Sections 922 and/or Title 22, United States Code, Sections 2778 exists on the Device and that the probable cause is sufficient for a warrant to search the Device and seize the items described in Attachment A.

Respectfully submitted,



Jesse L. Axley
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on June 16, 2017:



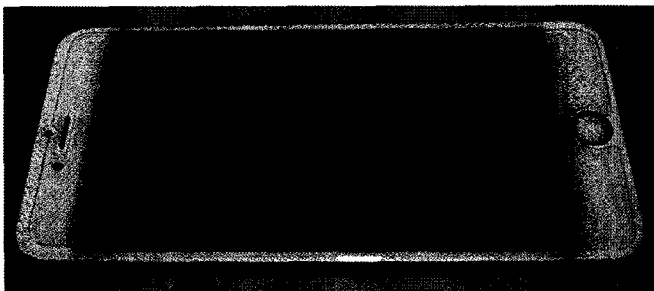
Ignacio Torteya, III
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

B-17-554-MJ

One (1) Apple iPhone Model A1687, IMEI# 355729075698832 and Serial Number: F2LT5ATSHFM5, rose gold in color, which was located and seized from Emmanuel RAVELL, on May 17, 2017, that relate to violations of Title 18, United States Code, Sections 922 and/or Title 22, United States Code, Sections 2778, which involve RAVELL and or Co-Conspirators, including:

1. The phone numbers and/or direct connect and/or names and identities, including electronic mail addresses, usernames and passwords assigned to the device;
2. Digital, cellular, and/or telephone numbers and/or direct connect numbers, names and identities, including electronic mail addresses, usernames and passwords stored in the device and in any other electronic media attached to or found with the device, including but not limited to SIM cards and flash memory cards;
3. Phone numbers, direct connect numbers, electronic mail addresses. Internet Protocol addresses and other accounts dialed or accessed using the Device or otherwise communicating with or accessing the device;
4. Photographs, text messages, electronic mail messages and any other documents or information stored in the device's memory relating to violations of Title 18, United States Code, Sections 922 and/or Title 22, United States Code, Sections 2778.
 - a. types, amounts, and prices of arms and munitions trafficked as well as dates, places, and amounts of specific transactions;
 - b. any information related to sources of arms and munitions (including names, addresses, phone numbers, or any other identifying information);
 - c. any information recording RAVELL and or Co-Conspirators' schedule or travel;
 - d. all bank records, checks, credit card bills, account information, and other financial records.
5. Evidence of user attribution showing who used or owned the cellular phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.



ATTACHMENT A

B-17-554-MJ

One (1) Apple iPhone Model A1687, IMEI# 355729075698832 and Serial Number: F2LT5ATSHFM5, rose gold in color, which was located and seized from Virginia Kimberly Aramburu, on May 17, 2017, that relate to violations of Title 18, United States Code, Sections 922 and/or Title 22, United States Code, Sections 2778, which involve Emmanuel RAVELL and or Co-Conspirators, including:

1. The phone numbers and/or direct connect and/or names and identities, including electronic mail addresses, usernames and passwords assigned to the device;
2. Digital, cellular, and/or telephone numbers and/or direct connect numbers, names and identities, including electronic mail addresses, usernames and passwords stored in the device and in any other electronic media attached to or found with the device, including but not limited to SIM cards and flash memory cards;
3. Phone numbers, direct connect numbers, electronic mail addresses. Internet Protocol addresses and other accounts dialed or accessed using the device or otherwise communicating with or accessing the device;
4. Photographs, text messages, electronic mail messages and any other documents or information stored in the device's memory relating to violations of Title 18, United States Code, Sections 922 and/or Title 22, United States Code, Sections 2778.
 - a. types, amounts, and prices of arms and munitions trafficked as well as dates, places, and amounts of specific transactions;
 - b. any information related to sources of arms and munitions (including names, addresses, phone numbers, or any other identifying information);
 - c. any information recording RAVELL and or Co-Conspirators' schedule or travel;
 - d. all bank records, checks, credit card bills, account information, and other financial records.
5. Evidence of user attribution showing who used or owned the cellular phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

